

Oracle Critical Patch Updates Unwrapped

Stephen Kost
Integrigy Corporation
Session # 120

Introduction

- **Stephen Kost**

- Chief Technology Officer of Integrigy Corporation
- 12 years experience with Oracle Database as database administrator, architect, and security researcher
- Found more than 50 security bugs fixed in CPUs

- **Integrigy Corporation**

- Dedicated to Oracle Security
- Services – Oracle Security Assessments
- Products – AppSentry and AppDefend

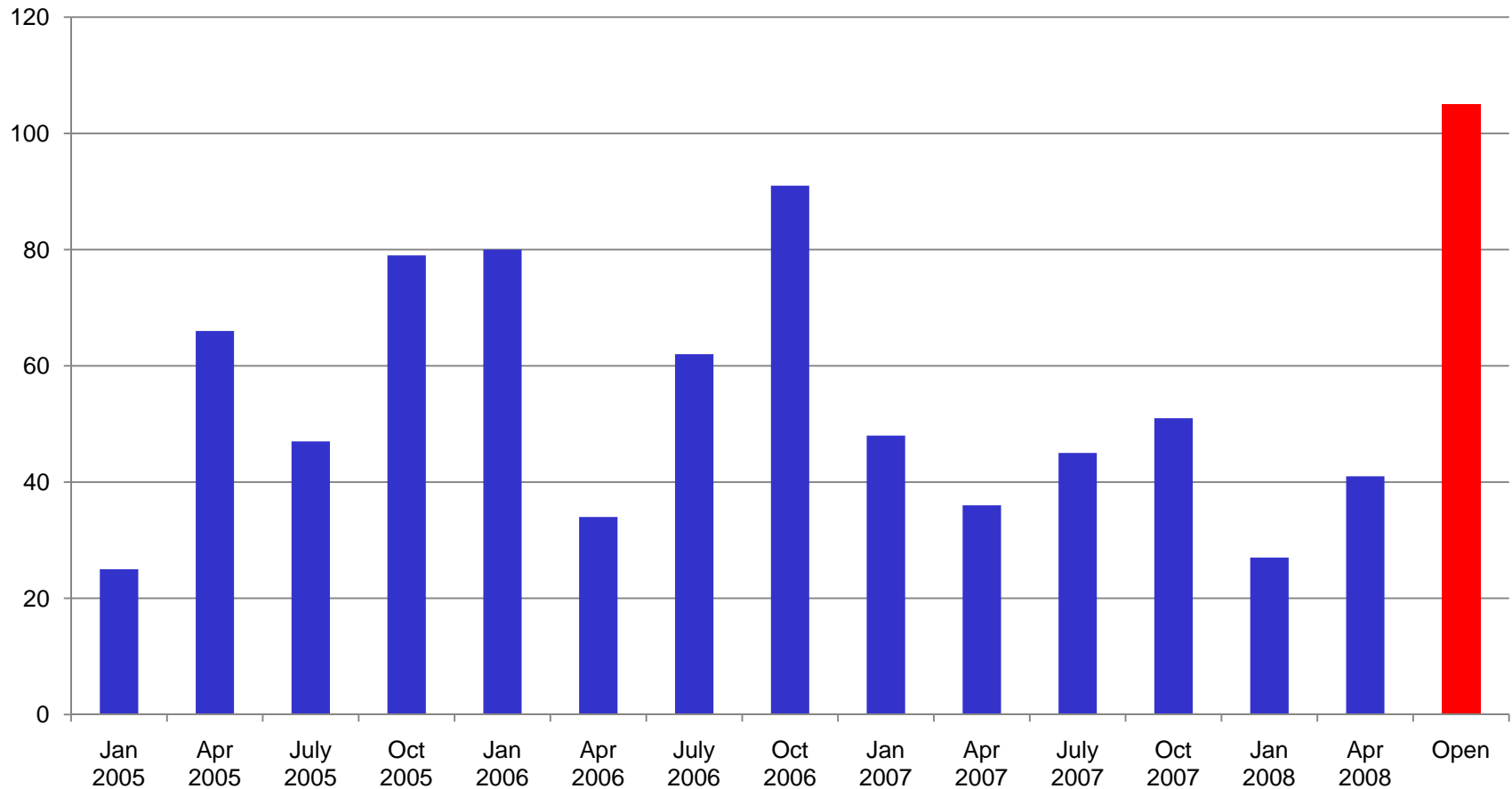
Agenda

- Background of Critical Patch Updates
- Vulnerabilities
- Certification vs. Certification
- Patches
- Questions

Oracle Critical Patch Updates

- Fixes for security bugs in all Oracle products
 - Released quarterly on a fixed schedule
 - Tuesday closest to the 15th day of January, April, July and October
 - Next CPUs = April 15, 2008 (yesterday) and July 15, 2008
- Fourteen CPUs released to date starting with January 2005
 - 732 security bugs fixed (average is 53 bugs per CPU)
 - 323 bugs in the Oracle Database

Security Bugs per CPU (all products)



Security Bug Process

Bug reported

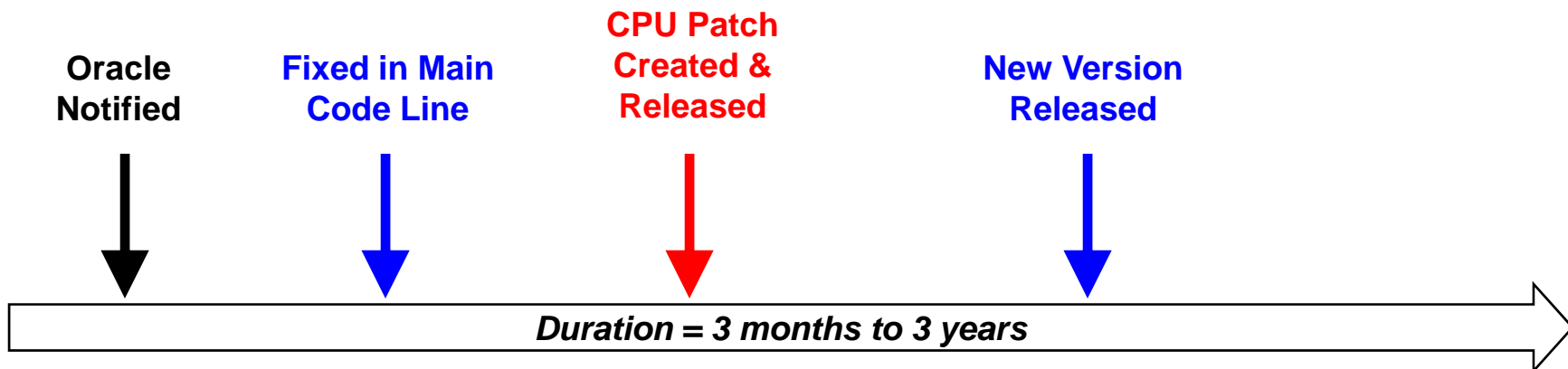
1. Customer or security researcher reports security bug to Oracle
2. Oracle researches bug and develops bug fix
 - Finder not allowed to test fix or even notified about fix
3. Oracle fixes in main code line
 - May include fix in new releases
 - No notification of security fixes to customers
4. Oracle back-ports fix for quarterly CPU
 - April 2008 CPU is 56 database patches
 - **From initial report to security patch release is 3 months to 3 years**

Elapsed time on average is 18 months

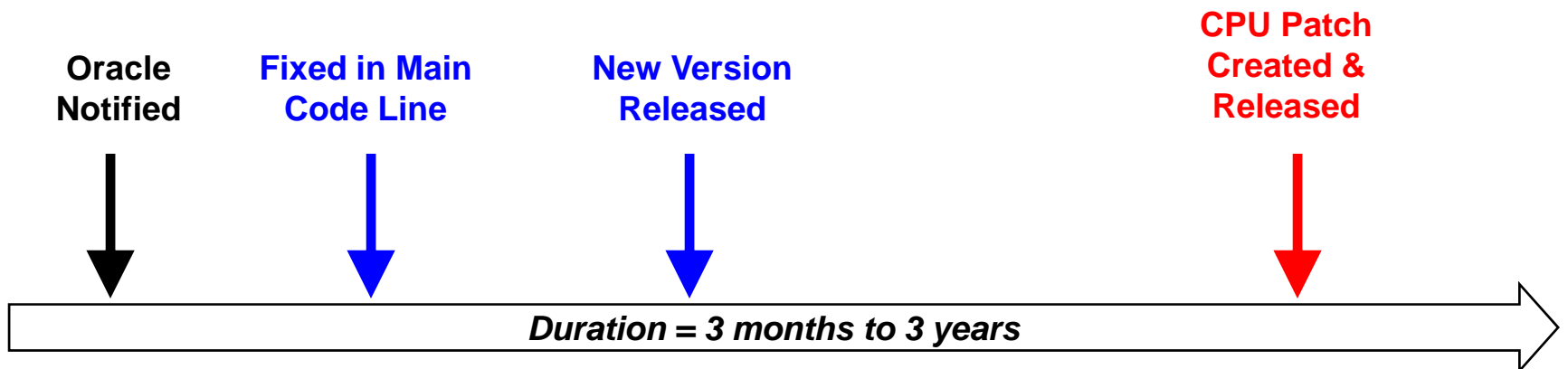
Bug fixed

- Vulnerability may be fixed first in a new version (e.g., 10.2.0.4) before through a Critical Patch Update with no notification

Scenario A



Scenario B



Oracle and CVSS

- CVSS = Common vulnerability Scoring System
 - A common scoring for the risk and severity of vulnerabilities - base metric score is 1 to 10 (10=worst)
 - Designed for network devices and servers, not databases and applications – biased toward root access
- ***Oracle CVSS base metric scores will always be low***
 - A problem with the metric, not Oracle
- Oracle Database realistic maximum is **5.5 to 6.5**
- **Oracle includes “Partial+” in the advisory**

Types of Oracle Security Bugs

- Buffer Overflow
- SQL Injection
- Cross-site Scripting (XSS)
- Parameter Tampering
- Permission Issues
- Information Disclosure

% of Bugs Exploitable with No Auth

4%

For the CPUs January 2007 through January 2008 (3 of 81 database bugs)

% of Bugs PUBLIC Exploitable

44%

% of Published Exploits PUBLIC Exploitable

89%

For the CPUs January 2007 through January 2008 (16 of 18 database bugs)

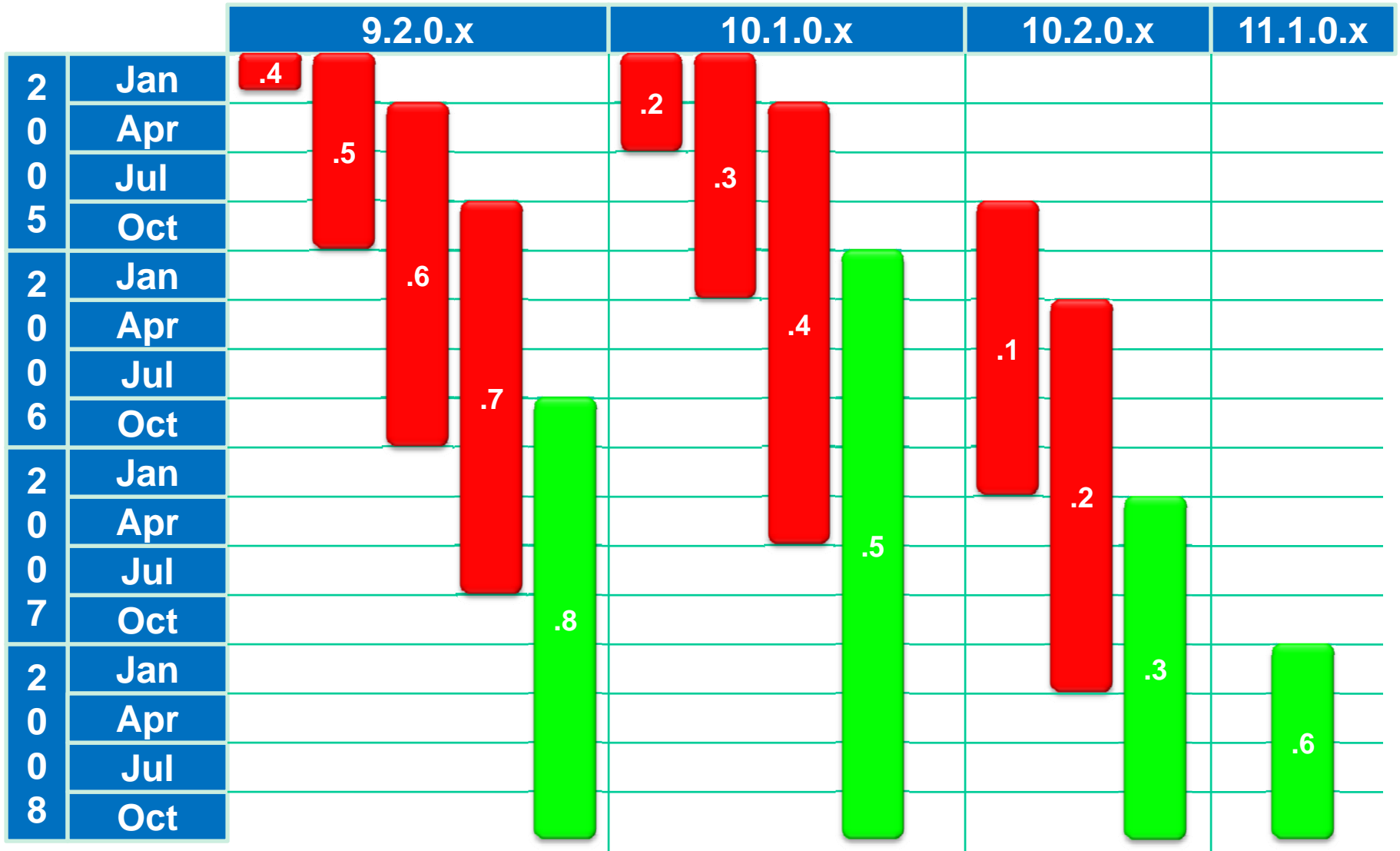
Database Vulnerabilities (Jan08)

Supported Database Version	PUBLIC (i.e., any database account)	Other Privileges (CREATE VIEW)	No Default Privileges
9.2.0.8	DB04 – SDO_CATALOG DB06 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.1.0.5	DB04 – SDO_CATALOG DB06 – Oracle Spatial DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM DB03 - DBMS_PRVTAQIP
10.2.0.3	DB04 – SDO_CATALOG DB07 – Oracle Spatial	DB01 – XML DB	DB02 - DBMS_PRVTAQIM

Metalink Certification != CPU Certification

- **Oracle Software Error Correction Support Policy**
- **Last two patches released in the **past 1 year****

“As a general rule, Critical Patch Updates (CPUs) are created for the last two patch sets of Server Technologies releases during the period when a release is in Premier Support (under the Lifetime Support Policy) or Error Correction Support (ECS). However, in the case where the latest patch set of a release has been available for more than 1 year, CPUs will be provided only for the most recent patch set for that release. Once a release enters its Extended Support (under the Lifetime Support Policy) or Extended Maintenance Support (EMS) period, CPUs are created only for the last patch set of that release.”



CPU Database Patch Differences

Version

10.2.0.3 and higher

Beginning with 10.2.0.3, Oracle introduced the n-apply CPU patching allowing for partial application of patch if a conflict exists.

With 10.2.0.3 and higher, CPU patches will only include security related fixes and necessary pre-requisites. Previously, CPU patches may have included high priority non-security fixes.

Operating System

Windows vs. Unix/Linux

Windows CPU database patches are patch bundles which include non-security related fixes.

n-apply CPU - Molecules

- Introduced with July 2007 CPU for 10.2.0.3 and higher
- Each security fix is a molecule
 - **If cumulative molecule is already applied, it is skipped (only for ORACLE_HOME)**
 - Allows better handling of patch conflicts through standard merge patches
 - Optionally, CPU patch can be partially applied while waiting to receive a merge patch (“partial n-apply”)
 - For some versions, merge patches must be requested within less than 3 weeks

Checking CPU Patches

- OPatch Inventory

```
opatch lsinventory -detail | grep -i cpu
```

- Database

```
select * from SYS.REGISTRY$HISTORY
```

- REGISTRY\$HISTORY populated with January 2006 CPU
- Previous CPU information deleted

- **Neither method guarantees CPU was successfully or completely applied**

Other CPU Issues

- CPU is two parts (1) Oracle Home Files and (2) Database Objects (catcpu.sql)
 - When creating a new database from a patched Oracle Home, must apply catcpu.sql to the new database
- CPU database patches may undo some security hardening changes, such as re-applying grants to PUBLIC on SYS objects
- Oracle Configuration Manager (OCM) is now installed as part of some CPU database patches

References

- Oracle, “Oracle Critical Patch Update April 2008 Advisory”, <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Oracle, “Critical Patch Update April 2008 Availability Information for Oracle Database and Fusion Middleware Products”, Metalink Note ID 552248.1
- Oracle, “Critical Patch Update - Introduction to Database n-Apply CPUs”, Metalink Note ID 438314.1
- Oracle, “Critical Patch Update Database Patch Security Vulnerability Molecule Mapping for April 2008 CPU”, Metalink Note ID 552253.1
- Oracle, “Security Alerts and Critical Patch Updates- Frequently Asked Questions”, Metalink Note ID 360470.1
- Oracle, “Database, FMW, and OCS Software Error Correction Support Policy Version 2.1”, Metalink Note ID 209768.1

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

E-mail: skost@integrigy.com
Phone: 312-961-0215

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681
888/542-4802

Website: www.integrigy.com
Sales: sales@integrigy.com
Development: development@integrigy.com
Support: support@integrigy.com
Security Alerts: alerts@integrigy.com

Questions?